Course CT-300 – 5 days -Instructor-led

CompTIA Security+ Certification

Introduction

Security+™: A CompTIA Certification (Windows Server 2003) is the primary course you will need to take if your job responsibilities include securing network services, network devices, and network traffic. It is also the main course you will take to prepare for the CompTIA Security+ examination (exam number SY0-101). In this course, you'll build on your knowledge and professional experience with computer hardware, operating systems, and networks as you acquire the specific skills required to implement basic security services on any type of computer network.

At Course Completion

Upon successful completion of this course, students will be able to:

- identify fundamental concepts of computer security.
- identify security threats.
- harden internal systems and services.
- harden internetwork devices and services.
- secure network communications.
- manage public key infrastructure (PKI).
- manage certificates.
- enforce organizational security policies.
- monitor the security infrastructure.

Prerequisites

- Basic Windows skills and fundamental understanding of computer and networking concepts are required.
- CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months experience in networking, including experience configuring and managing TCP/IP, are strongly recommended.
- Additional introductory courses in operating system administration for Windows, UNIX, Linux, or NetWare are helpful but not required.

Certification Exams

- This course will help prepare students to achieve a CompTIA Security+ Certification.

Course Materials and Software

- Security+: A CompTIA Certification (Windows Server 2003). ElementK Courseware, 2006

Course Outline

Lesson 1: Security Fundamentals
        Topic 1A: Security Building Blocks
        Topic 1B: Authentication Methods
        Topic 1C: Cryptography Fundamentals
        Topic 1D: Security Policy Fundamentals

Lesson 2: Security Threats
        Topic 2A: Social Engineering
        Topic 2B: Software-Based Threats
        Topic 2C: Hardware-Based Threats

Lesson 3: Hardening Internal Systems and Services
        Topic 3A: Harden Operating Systems
        Topic 3B: Harden Directory Services
        Topic 3C: Harden DHCP Servers
        Topic 3D: Harden File and Print Servers

Lesson 4: Hardening Internetwork Devices and Services
        Topic 4A: Harden Internetwork Connection Devices
        Topic 4B: Harden DNS and BIND Servers
        Topic 4C: Harden Web Servers
        Topic 4D: Harden File Transfer Protocol (FTP) Servers
        Topic 4E: Harden Network News Transfer Protocol (NNTP) Servers
        Topic 4F: Harden Email Servers
        Topic 4G: Harden Conferencing and Messaging Servers

Lesson 5: Securing Network Communications
        Topic 5A: Protect Network Traffic with IP Security (IPSec)
        Topic 5B: Secure Wireless Traffic
        Topic 5C: Harden a Web Browser
        Topic 5D: Secure the Remote Access Channel

Lesson 6: Managing Public Key Infrastructure (PKI)
        Topic 6A: Install a Certificate Authority (CA) Hierarchy
        Topic 6B: Harden a Certificate Authority
        Topic 6C: Back Up a CA
        Topic 6D: Restore a CA

Lesson 7: Managing Certificates
  Topic 7A: Enroll Certificates
  Topic 7B: Secure Network Traffic by Using Certificates
  Topic 7C: Renew Certificates
  Topic 7D: Revoke Certificates
  Topic 7E: Back Up Certificates and Private Keys
  Topic 7F: Restore Certificates and Private Keys

Lesson 8: Enforcing Organizational Security Policies
  Topic 8A: Enforce Corporate Security Policy Compliance
  Topic 8B: Enforce Legal Compliance
  Topic 8C: Enforce Physical Security Compliance
  Topic 8D: Educate Users

Lesson 9: Monitoring the Security Infrastructure
  Topic 9A: Scan for Vulnerabilities
  Topic 9B: Monitor for Intruders
  Topic 9C: Set Up a Honeypot
  Topic 9D: Respond to Security Incidents

Appendix A: Mapping Security+ Course Content to the CompTIA Security+ Exam Objectives

Appendix B: Using Security Utilities